REMARKS

Claims 1-4 and 15 are pending. Claims 5-14 and 16 have been withdrawn. Applicant has amended claims 1 and 15 herein.

The Examiner has made the restriction requirement final. Applicant reserves the right to file a petition for review of the restriction later under 37 C.F.R. § 1.144.

The Examiner rejected claim 15 under 35 U.S.C. § 101 as being directed to nonstatutory subject matter, because it is a data structure claim. Data structures embodied in computer-readable media are statutory subject matter. According to M.P.E.P. § 2106(IV)(B)(1)(a):

> [A] claimed computer-readable medium encoded with a *data structure* defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. (Emphasis added.)

Applicant has amended claim 15 to clarify that the data structure is encoded in a computer-readable medium. Claim 15 as amended recites a "computer-readable medium encoded with a data structure." Applicant's claimed technology meets the requirements of the above-quoted section, and thus is directed to statutory subject matter. Accordingly, Applicant respectfully requests that this rejection be withdrawn.

The Examiner rejected claim 15 under 35 U.S.C. § 102(b) over Baugher ("The Secure Real-time Transport Protocol") and claims 1-4 under 35 U.S.C. § 103(a) over Baugher in view of Minhazuddin (2004/0073641). Applicant respectfully traverses these rejections.

Baugher describes a protocol, called SRTP, for securing communications sent in accordance with the Real-time Transport Protocol (RTP). Like RTP itself, SRTP relies on a unique destination address and port for each receiving client. Baugher states, "[a] cryptographic context SHALL be uniquely identified by the triplet context identifier: context

id = <SSRC, destination network address, destination transport port number>" and "[i]t is assumed that, when presented with this information, the key management returns a context with the [cryptographic context] information." Baugher, p. 9. However, in many situations, particularly where firewalls are involved, the number of available destination ports is severely limited such that it is not possible or desirable to give each receiving client a unique destination port. Thus, the assumption stated in Baugher is false for these situations because a destination address and port are insufficient to uniquely identify a particular context, even if combined with the SSRC value. Baugher does not address these situations and contains no teaching or suggestion of a method of handling the routing of RTP packets when the destination address and port are not unique.

In contrast, applicant's technology is directed to routing secure RTP traffic in an environment where destination ports are limited, such as a firewall. A firewall may contain a single IP address that is shared by many receiving clients. From a sender's point of view outside of the firewall, each of the receiving clients has the same destination address. If the firewall only allows RTP communications to be received on a particular port, then each of the receiving clients also appears to the sender to have the same destination port. Thus, when a packet is received, there is no way provided by RTP for the firewall to determine which receiving client should receive the packet. Applicant's technology observes that the sender's information can be made unique in these situations, and uses the sender's information to determine which receiving client should receive the packet.

In the embodiments of claims 1-4, applicant's technology distinguishes receiving clients based on the sender's source information in the RTP header. Applicant has amended claim 1 to clarify that the "source information" refers to the sender. Claim 1 as amended recites "determining whether a sending client's Security Association (SA) exists using the sender's source information included in the RTP message header" and "forwarding the packet to a receiving network client identified based on the sender's source information." In the embodiment of claim 15, applicant's technology distinguishes receiving clients based on a sender-provided Synchronization Source Identifier. Claim 15 recites

"wherein a receiving media relay server can determine a receiving client associated with the data structure based on the unencrypted Synchronization Source Identifier without identifying a unique port for the receiving client." Thus, each of applicant's pending claims describes distinguishing receiving clients without relying on a unique destination address and port. As discussed above, Baugher assumes a unique destination address and port for each receiving client and does not teach or suggest distinguishing receiving clients on any other basis. Minhazuddin, relied upon by the Examiner for teaching decrypting packets at a server, also does not teach or suggest distinguishing receiving clients where each receiving client does not have a unique destination address and port. Therefore, applicant's claims are patentable over Baugher alone and in combination with Minhazuddin. Accordingly, applicant respectfully requests that these rejections be withdrawn.

Based upon these remarks and amendments, Applicants respectfully request reconsideration of this application and its early allowance. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-3265. Applicants believe all required fees are being paid in connection with this response. However, if an additional fee is due, please charge our Deposit Account No. 50-0665, under Order No. 418268874US from which the undersigned is authorized to draw.

Dated: 9/5/2007

Respectfully submitted,

By _____
J. Mason Boswell
Registration No.: 58,388
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000
(206) 359-7198 (Fax)
Attorneys for Applicant